

# A MULTI-FREY APPROACH TO FERMAT EQUATIONS OF SIGNATURE $(r, r, p)$

NICOLAS BILLEREY, IMIN CHEN, LUIS DIEULEFAIT, AND NUNO FREITAS

ABSTRACT. In this paper, we give a complete resolution of the generalized Fermat equations

$$x^5 + y^5 = 3z^n \text{ and } x^{13} + y^{13} = 3z^n,$$

for all integers  $n \geq 2$ , using the modular method with Frey elliptic curves over totally real fields. The results require a refined application of the multi-Frey technique, which we show to be effective in new ways to reduce the bounds on the exponents  $n$ .

We also give a number of results for the equations  $x^5 + y^5 = dz^n$ , where  $d = 1, 2$ , under additional local conditions on the solutions. This includes a result which is reminiscent of the second case of Fermat's Last Theorem, and which uses a new application of level raising at  $p$  modulo  $p$ .

## 1. INTRODUCTION

Wiles' 1995 proof [41] of Fermat's Last Theorem pioneered a new strategy to attack Diophantine equations, now known as *the modular method*. The strategy, originally due to Frey, Serre, Ribet and Wiles is to attach to a putative solution of a Diophantine equation an elliptic curve  $E$  (known as a Frey curve), and study the mod  $p$  representation attached to  $E$  via modularity and level lowering. This relates the solution to a modular form of weight 2 and small level and, to conclude, one needs to show that such relation leads to a contradiction (see Section 2 for more details).

The idea of using this same strategy to study variants of FLT goes back to the work of Serre [40, Section 4.3] and Ribet [39]. Since Wiles' breakthrough, mathematicians have generalized and improved the method and applied it to many other Diophantine equations. In particular, it was natural to use the modular approach to study the *Generalized Fermat Equation*

$$(1.1) \quad Ax^p + By^q = Cz^r, \quad p, q, r \in \mathbb{Z}_{\geq 2}, \quad A, B, C \in \mathbb{Z}_{\neq 0}$$

with  $A, B, C$  pairwise coprime. This equation is subject of the following conjecture.

**Conjecture.** Fix  $A, B, C$  as above. Over all choices of prime exponents  $p, q, r$  satisfying  $1/p + 1/q + 1/r < 1$  the equation (1.1) admits only finitely many solutions  $(a, b, c)$  such that  $abc \neq 0$  and  $\gcd(a, b, c) = 1$ . (Here solutions like  $2^3 + 1^q = 3^2$  are counted only once.)

The only general result towards the above conjecture is a theorem due to Darmon and Granville [19] which states that if besides  $A, B, C$  we also fix the prime exponents  $p, q, r$  then

---

*Date:* March 21, 2017.

2010 *Mathematics Subject Classification.* Primary 11D41; Secondary 11F80, 11G05.

*Key words and phrases.* Fermat equations, modular method, multi-Frey.

N.B. acknowledges the financial support of ANR-14-CE-25-0015 Gardio. The last author was partly supported by the grant *Proyecto RSME-FBBVA 2015 José Luis Rubio de Francia*.

there are only finitely many solutions as above. The conjecture is also known to hold in some particular cases including certain infinite families, for which the authors of this paper have previously made contributions. Moreover, it is also known that the full conjecture is a consequence of the *ABC*-conjecture (see [19, Section 5.2]).

Bennett [2], [3], Kraus [33], [34] and Siksek [13], [14] and their collaborators have developed and clarified the method using Frey elliptic curves over  $\mathbb{Q}$ . Unfortunately, there is a restrictive set of exponents  $(p, q, r)$  which can be approached using the modular method over  $\mathbb{Q}$  due to constraints coming from the classification of Frey representations [19]. As a consequence, attention has now shifted towards using Frey elliptic curves over totally real fields, and is made possible because of advances on the Galois representation side (i.e. modularity results).

In this paper, we establish further cases of the conjecture above based on extensions of the modular method to the setting of Hilbert modular forms as introduced in the work of the last two authors [22], and powered by the multi-Frey technique as explained by Siksek in [15], [12].

The results in this paper provide evidence that the multi-Frey technique applied with a ‘sufficiently rich’ set of Frey curves can be used to ‘patch together’ a complete resolution of a one parameter family of generalized Fermat equations. As it will be seen throughout the paper, the multi-Frey technique complements methods used in several steps in the modular method, allowing for refined bounds.

**1.1. Our Diophantine results.** Let  $d \geq 1$  be an integer. We are concerned with Fermat type equations of the form

$$(1.2) \quad x^r + y^r = dz^p, \quad xyz \neq 0, \quad \gcd(x, y, z) = 1$$

where  $r, p$  are prime exponents with  $r$  fixed and  $p$  is allowed to vary.

We say that a solution  $(x, y, z) = (a, b, c)$  of equation (1.2) is *non-trivial* if it satisfies  $|abc| > 1$  and we call it *primitive* if  $\gcd(a, b, c) = 1$ . In the case of most interest to us,  $d = 3$ , the condition  $|abc| > 1$  is equivalent to  $abc \neq 0$ , but it is important to note that for  $d = 2$  there are also the extra trivial solutions  $\pm(1, 1, 1)$ .

The equation (1.2) with  $r = 5$  and  $d = 2, 3$  has already been subject of the papers [5], [7] and [23], where it was resolved for 3/4 of prime exponents  $p$ . For  $r = 13$  and  $d = 3$ , it has been resolved in the papers [22], [28] under the assumption  $13 \nmid z$ .

Our main Diophantine results are that we completely solve equation (1.2) for  $d = 3$  when  $r = 5, 13$  and  $p = n \geq 2$  is any integer. Clearly, this will follow directly from the same statements for prime exponents. More precisely, we will prove the following theorems.

**Theorem 1.** *For all primes  $p$ , there are no non-trivial primitive solutions to*

$$(1.3) \quad x^5 + y^5 = 3z^p.$$

**Theorem 2.** *For all primes  $p$ , there are no non-trivial primitive solutions to*

$$(1.4) \quad x^{13} + y^{13} = 3z^p.$$

In the previous papers concerning equations (1.3) and (1.4), the main tool used was the modular method, where the Frey curves were obtained by exploiting the factorization over  $\mathbb{Q}(\zeta_r)$  (for  $r = 5$  or  $r = 13$ ) of the left-hand side of each equation. More generally, in the work of the last author [26], for each  $r \geq 5$ , several Frey curves defined over real subfields of  $\mathbb{Q}(\zeta_r)$  are attached to equation (1.2). Our proofs of Theorems 1 and 2 build on these previous works and are made possible by introducing new multi-Frey techniques.

In particular, we show how the multi-Frey technique can be used to obtain tight bounds on the exponent  $p$ , improve bounds coming from Mazur-type irreducibility results (see Proposition 1 and Theorem 8), and move to another level where the required computations of Hilbert modular forms is within the range of what is currently feasible (see paragraph after Lemma 5). We also need a refined ‘image of inertia argument’ (see Section 3) for the elimination step of the modular method.

A major obstruction to the success of the modular method for solving (1.2) for  $d = 1, 2$  is the existence of trivial solutions like  $(1, 0, 1)$ ,  $(1, -1, 0)$  or  $(1, 1, 1)$ . Indeed, when the Frey curve evaluated at a trivial solution is non-singular then its corresponding (via modularity) newform will be among the newforms after level lowering; in particular, the mod  $p$  representations of the Frey curve and a newform can be isomorphic, requiring the use of global methods to distinguish Galois representations which are uniform in  $p$ .

It is sometimes possible to resolve equation (1.2) by assuming additional  $q$ -adic conditions to avoid the obstructing trivial solutions. Indeed, we will prove a number of partial results for the equation (1.2) with  $r = 5$  and  $d = 1, 2$  under certain  $q$ -adic conditions.

For example, we will prove the following result resembling the second case of Fermat’s Last Theorem. Its proof involves a new application of the condition for level raising at  $p$  modulo  $p$ .

**Theorem 3.** *For all primes  $p$ , the equation*

$$x^5 + y^5 = dz^p, \quad \text{with } d \in \{1, 2\}$$

*has no non-trivial solutions  $(a, b, c)$  satisfying  $p \mid c$ .*

In addition, we will use the multi-Frey technique to prove the following result.

**Theorem 4.** *For all primes  $p$ , the equation*

$$x^5 + y^5 = dz^p$$

*has no non-trivial solutions  $(a, b, c)$  in each of the following situations :*

- (i)  $d = 1, 2$  and  $5 \mid c$  or,
- (ii)  $d = 1$  and  $c$  even or,
- (iii)  $d = 2$  and  $c$  even.

We remark that, in all our theorems, to deal with certain small primes, we invoke references where the results are obtained using Frey curves different from the ones used in this paper; this is another instance of the multi-Frey technique.

The computations required to support the proof of our main theorems were performed using **Magma** [8]. The program files are provided with this paper and we refer to [6] whenever an assertion involves a computation in **Magma** from one of these programs.

**Acknowledgments.** We thank Christophe Breuil for discussions concerning Proposition 6. We also thank Peter Bruin for helpful conversations regarding Remark 7.8 and Maarten Derickx and Michael Stoll for a conversation about [21].

## 2. OVERVIEW OF THE MULTI-FREY MODULAR METHOD

**Notation:** Let  $\overline{\mathbb{Q}}$  be an algebraic closure of  $\mathbb{Q}$  and let  $p$  be a prime number. For a totally real subfield  $K$  of  $\overline{\mathbb{Q}}$ , we write  $G_K = \text{Gal}(\overline{\mathbb{Q}}/K)$  for its absolute Galois group. For a prime  $\ell$  of  $K$  we write  $I_\ell$  for an inertia subgroup at  $\ell$  in  $G_K$ . Given  $E$  an elliptic curve defined over  $K$ , we denote by  $\overline{\rho}_{E,p}$  the representation giving the action of  $\text{Gal}(\overline{\mathbb{Q}}/K)$  on the  $p$ -torsion points of  $E$ . For a Hilbert modular form  $f$  defined over  $K$  and a prime ideal  $\mathfrak{p}$  in its field of coefficients  $\mathbb{Q}_f$ , we write  $\overline{\rho}_{f,\mathfrak{p}}$  for the mod  $\mathfrak{p}$  Galois representation attached to  $f$ ; when  $K = \mathbb{Q}$  we get classical modular forms.

We now recall the main steps of the modular method.

**Step 1: Constructing a Frey curve.** Attach a Frey elliptic curve  $E/K$  to a putative solution of a Diophantine equation, where  $K$  is a totally real field. A Frey curve  $E/K$  has the property that the Artin conductor of  $\overline{\rho}_{E,p}$  is bounded independently of the putative solution.

**Step 2: Modularity.** Prove the modularity of  $E/K$ , and hence modularity of  $\overline{\rho}_{E,p}$ .

**Step 3: Irreducibility.** Prove the irreducibility of  $\overline{\rho}_{E,p}$ .

**Step 4: Level lowering.** Use level lowering theorems, which require irreducibility of  $\overline{\rho}_{E,p}$ , to conclude that  $\overline{\rho}_{E,p} \cong \overline{\rho}_{f,\mathfrak{p}}$  where  $f$  is a Hilbert newform over  $K$  of parallel weight 2, trivial character, and level among finitely many explicit possibilities  $N_i$  and  $\mathfrak{p}$  is a prime ideal above  $p$  in the field of coefficients  $\mathbb{Q}_f$  of  $f$ .

**Step 5: Contradiction.** Compute all the Hilbert newforms predicted in Step 4 and show that  $\overline{\rho}_{E,p} \not\cong \overline{\rho}_{f,\mathfrak{p}}$  for all of them. This typically uses various methods to distinguish local Galois representations.

In current applications of the modular method, the most challenging step is often Step 5, contrasting with the proof of Fermat's Last Theorem (the origin of the modular method) where the big issue was modularity. Indeed, in the proof of FLT we have  $K = \mathbb{Q}$  and in Step 4 there is only one level  $N_1 = 2$ ; since there are no newforms at this level we get directly a contradiction in Step 5. In essentially every other application of the method, there are candidates for  $f$ , therefore more work is needed to complete the argument, namely Step 5. It is now convenient for us to divide Step 5 into two substeps.

**Step 5a: Computing newforms.** Compute all the Hilbert newforms of parallel weight 2, trivial character and levels  $N_i$  predicted in Step 4.

**Step 5b: Discarding newforms.** For each newform  $f$  computed in Step 5a and each prime ideal  $\mathfrak{p}$  above  $p$  in its field of coefficients show that  $\overline{\rho}_{E,p} \not\cong \overline{\rho}_{f,\mathfrak{p}}$ .

With the objective of succeeding more often in Step 5, Siksek introduced the **multi-Frey technique** in [15] and [12]. This is a variant of Step 1 where more than one Frey curve is used simultaneously in order to put more restrictions on the putative solutions, thereby increasing the likelihood of a contradiction in Step 5b.

It is a common assumption in discussions about the modular method found in the literature that Step 5a can be completed. We want to stress that more recently Step 5a is becoming a real obstruction to the method. This computational obstruction was not noticed in initial applications since they only required small (even empty) spaces of newforms over  $\mathbb{Q}$  which were easily accessible. However, when working over totally real fields this is no longer the case as the dimensions of spaces of Hilbert cusp forms grow very fast.

Besides the Diophantine results mentioned in the Introduction, one of the underlying themes of this paper is to illustrate that the multi-Frey approach is a powerful and versatile tool with applications at various stages of the modular method. Indeed, in the proofs of our main results, we will use it to circumvent challenges in Steps 3, 5a, and 5b.

### 3. THE IMAGE OF INERTIA ARGUMENT

In this section we recall and generalize the ‘image of inertia argument’, which is a technique to distinguish local Galois representations, and is used in Step 5b of the modular method. We start with the well known version, and then provide two generalizations. All three versions are used later in the paper.

**Notation.** Let  $F$  be a finite extension of  $\mathbb{Q}_\ell$  contained in some fixed algebraic closure  $\overline{\mathbb{Q}_\ell}$  of  $\mathbb{Q}_\ell$ . Let  $E/F$  be an elliptic curve with potentially good reduction. Let  $m \in \mathbb{Z}_{\geq 3}$  be coprime to  $\ell$  and consider the *inertial field* of  $E$  given by  $L_E = F^{un}(E[m])$ , where  $F^{un}$  is the maximal unramified extension of  $F$  in  $\overline{\mathbb{Q}_\ell}$ . The extension  $L_E/F^{un}$  is independent of  $m$  and it is the minimal extension of  $F^{un}$  where  $E$  achieves good reduction.

Suppose that, for a prime  $p$ , we have

$$(3.1) \quad \overline{\rho}_{E,p} \cong \overline{\rho}_{Z,p},$$

where  $E$  and  $Z$  are elliptic curves over a local field  $F$ . In our applications below  $E$  and  $Z$  will be defined over a totally real number field  $K$  and  $F$  will be the completion of  $K$  at some prime  $\ell$ . Moreover,  $E$  will be a Frey curve and  $Z$  an elliptic curve corresponding to a (Hilbert) newform with rational coefficients, predicted in Step 4 of the modular method. The objective of the inertia argument is to obtain a contradiction to (3.1), therefore establishing

$$(3.2) \quad \overline{\rho}_{E,p} \not\cong \overline{\rho}_{Z,p},$$

as required in Step 5b. We will now describe the three versions, each version generalizing the previous one.

**Version 1: different inertia sizes.** Show that  $\#\overline{\rho}_{E,p}(I_\ell) \neq \#\overline{\rho}_{Z,p}(I_\ell)$ ; this clearly implies (3.2). This is very effective when one curve has potentially good reduction and the other has potentially multiplicative reduction.

This version is very well known and it can be found in many papers on the modular method, including some of the older ones, for example [2].

**Version 2: the field of good reduction.** Suppose both  $E$  and  $Z$  have potentially good reduction. Note that the inertial field  $L_E$  corresponds to the field fixed by the restriction  $\overline{\rho}_{E,p}|_{I_\ell}$  and that isomorphism (3.1) implies  $\overline{\rho}_{E,p}|_{I_\ell} \cong \overline{\rho}_{Z,p}|_{I_\ell}$ . Then the inertial fields of  $E$  and  $Z$  must be the same. Therefore, even when  $\#\overline{\rho}_{E,p}(I_\ell) = \#\overline{\rho}_{Z,p}(I_\ell)$  (i.e. version 1 fails) we can

still establish (3.2) by showing that  $L_E$  and  $L_Z$  are not equal (working in a fixed algebraic closure of  $F$ ).

In practice, this is achieved by finding an extension  $M/F$  where  $E$  has good reduction and  $Z$  does not. Indeed, consider the compositum  $L = F^{un}M$ , which is an unramified extension of  $M$ . Therefore, the type of reduction of  $E$  and  $Z$  over  $L$  is the same as over  $M$ . Since  $E/L$  has good reduction by minimality of  $L_E$ , it follows  $L_E \subset L$ ; since  $Z/L$  does not have good reduction we have  $L_Z \not\subset L$ , and hence  $L_Z \neq L_E$ . We note that (when both curves have potentially good reduction) version 1 boils down to showing that  $L_E$  and  $L_Z$  are different because they have different degrees over  $F^{un}$ . This version was used in [1] for instance.

**Version 3: different conductors.** Let  $M$  be an extension of  $F$  and  $G_M \subset \text{Gal}(\overline{F}/F)$  its corresponding subgroup. Note that the isomorphism (3.1) implies that  $\overline{\rho}_{E,p}|_{G_M} \cong \overline{\rho}_{Z,p}|_{G_M}$ . In particular, the restrictions  $\overline{\rho}_{E,p}|_{G_M}$  and  $\overline{\rho}_{Z,p}|_{G_M}$  must have the same conductor. Therefore, we can establish (3.2) if we find a field  $M/F$  where the two restrictions have different conductors.

Note that version 2 is obtained by taking  $M = L_E$ . Indeed, we get  $G_M = I_\ell$  and  $\overline{\rho}_{E,p}|_{G_M}$  will have conductor exponent 0 (because  $E/M$  has good reduction) whereas  $\overline{\rho}_{Z,p}|_{G_M}$  has conductor exponent non-zero (because  $Z/M$  does not have good reduction).

*Remark 3.3.* In applications, the curves are often defined over a totally real number field  $K$ . Therefore, we can test if any of the versions above succeeds for different primes. Success at one prime is enough to discard the global isomorphism of two mod  $p$  representations.

*Remark 3.4.* We have explained the arguments above using elliptic curves, because this is the setting in which we will apply them. In principle, one could replace  $E$  and  $F$  by modular forms  $f$  and  $g$  and show that  $\overline{\rho}_{f,p} \not\cong \overline{\rho}_{g,p}$  using [36] and [37], but in practice it is harder to understand the action of inertia explicitly for modular forms.

#### 4. A MULTI-FREY APPROACH TO THE EQUATION $x^5 + y^5 = 3z^p$

In this section, we will use the following factorization and notation

$$x^5 + y^5 = (x + y)\phi_5(x, y) = (x + y)\psi_5(x, y)\bar{\psi}_5(x, y),$$

where  $\omega$  and  $\bar{\omega}$  are the complex roots of  $X^2 + X - 1$ , and

$$\begin{aligned}\phi_5(x, y) &= x^4 - x^3y + x^2y^2 - xy^3 + y^4 \\ \psi_5(x, y) &= x^2 + \omega xy + y^2, \quad \bar{\psi}_5(x, y) = x^2 + \bar{\omega} xy + y^2.\end{aligned}$$

**4.1. The modular method over  $\mathbb{Q}$ .** Here we compile results from [5] and [7].

Let  $p \geq 5$  be a prime number and let  $(a, b, c)$  be a solution to (1.2) with  $r = 5$ . We attach to it the following Frey elliptic curve over  $\mathbb{Q}$  denoted  $E(a, b)$  or  $E$  in [5] and [7], and whose construction is due to Darmon :

$$W_{a,b} : y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\phi_5(a, b)x.$$

The discriminant  $\Delta(W_{a,b})$  of  $W_{a,b}$  is given by

$$\Delta(W_{a,b}) = 2^4 5^3 (a + b)^2 (a^5 + b^5)^2.$$



Let  $W_0$  and  $W'_0$  be the rational elliptic curves defined by the following equations

$$W_0 : y^2 = x^3 + x^2 + 592x - 16812$$

and

$$W'_0 : y^2 = x^3 - x^2 - 333x - 2088.$$

They are labelled [35, 1200.k8] and [35, 1200.a1] in LMFDB respectively. In [5], the elliptic curves  $W_0$  and  $W'_0$  were referred to as 1200P1 and 1200N1 (in Cremona's labelling) respectively, whereas in [7] the authors used Stein's notation 1200K1 and 1200A1.

**Lemma 1.** *Let  $(a, b, c)$  be a non-trivial primitive solutions to (1.3) for  $p \geq 5$ . Then*

$$v_2(a) = 1 \quad \text{and} \quad p > 10^7.$$

*Furthermore,  $\bar{\rho}_{W,p} \cong \bar{\rho}_{W_0,p}$  or  $\bar{\rho}_{W,p} \cong \bar{\rho}_{W'_0,p}$  according to whether 5 divides  $a + b$  or not. Here,  $v_2(a)$  denotes the valuation at 2 of  $a$ .*

*Proof.* This follows from combining results from [5, Proposition 3.3], [7, Lemma 4.4] and [7, Remark 4.6].  $\square$

In our proof of Theorem 1, we will only make use of  $v_2(a) = 1$  and  $p \geq 11$ ; we included this more general statement here to make it clear what is the obstruction to the success of the modular method for solving equation (1.3) using the Frey curve  $W_{a,b}$ .

**4.2. The modular method over  $\mathbb{Q}(\sqrt{5})$ .** In [23], the modular method was applied with the multi-Frey technique using two Frey  $\mathbb{Q}$ -curves defined over  $\mathbb{Q}(\sqrt{5})$  to solve (1.3) for a set of prime exponents with Dirichlet density  $3/4$ . At the time, the purpose of using  $\mathbb{Q}$ -curves was to guarantee their modularity. It is now known that elliptic curves over real quadratic fields are modular (see [27]) and therefore we can work directly over  $\mathbb{Q}(\sqrt{5})$ , largely simplifying the arguments.

We now sharpen the relevant results from [23] in the language of Hilbert modular forms.

Let  $a, b$  be integers such that  $a^5 + b^5 \neq 0$ . Using the notation in the beginning of this section, we consider the two elliptic curves defined over  $\mathbb{Q}(\sqrt{5})$  by the following equations :

$$\begin{aligned} E_{a,b} : y^2 &= x^3 + 2(a+b)x^2 - \bar{\omega}\psi_5(a, b)x \\ F_{a,b} : y^2 &= x^3 + 2(a-b)x^2 + \left( \frac{-3(\omega - \bar{\omega})}{10} + \frac{1}{2} \right) \psi_5(a, b)x. \end{aligned}$$

These two curves were denoted  $E_{(a,b)}$  and  $F_{(a,b)}$  in [23], respectively. Using the equalities

$$\begin{aligned} (a+b)^2 &= -\bar{\omega}\psi_5(a, b) - \omega\bar{\psi}_5(a, b) \\ (a-b)^2 &= \left( \frac{-3}{10}(\omega - \bar{\omega}) + \frac{1}{2} \right) \psi_5(a, b) + \left( \frac{3}{10}(\omega - \bar{\omega}) + \frac{1}{2} \right) \bar{\psi}_5(a, b) \end{aligned}$$

we show that their discriminants are given by the following identities :

$$(4.1) \quad \Delta(E_{a,b}) = 2^6 \bar{\omega} \phi_5(a, b) \psi_5(a, b)$$

$$(4.2) \quad \Delta(F_{a,b}) = 2^6 \left( \frac{-3}{10}(\omega - \bar{\omega}) + \frac{1}{2} \right)^2 \left( \frac{3}{10}(\omega - \bar{\omega}) + \frac{1}{2} \right) \phi_5(a, b) \psi_5(a, b).$$

Let  $(a, b, c)$  be a primitive solution to (1.2) with  $r = 5$ , where  $d \geq 1$  is an integer such that all its prime factors  $\ell$  satisfy  $\ell \not\equiv 1 \pmod{5}$ .

Write  $E = E_{a,b}$  and  $F = F_{a,b}$ . Let  $\mathfrak{q}$  be a prime ideal in  $\mathbb{Q}(\sqrt{5})$  of residual characteristic  $\ell \neq 2, 5$  dividing  $\phi_5(a, b)\psi_5(a, b)$ . From the assumptions on  $a, b, c$  and  $d$ , using the results in [23], Sections 2 and 3, it follows that  $E$  and  $F$  have multiplicative reduction at  $\mathfrak{q}$  and that the valuation at  $\mathfrak{q}$  of  $\Delta(E)$  and  $\Delta(F)$  is divisible by  $p$ . From this, we conclude that the Artin conductor the mod  $p$  Galois representations attached to  $E$  and  $F$  can only be divisible by  $\mathfrak{q}_2$  and  $\mathfrak{q}_5$ , the unique primes in  $\mathbb{Q}(\sqrt{5})$  above 2 and 5, respectively. Since 2 is inert in  $\mathbb{Q}(\sqrt{5})$  we will write simply 2 for  $\mathfrak{q}_2$ .

We apply Tate's algorithm (using [6]) to determine the conductors  $N_E$  and  $N_F$  of  $E$  and  $F$ , respectively. In particular, we obtain :

$$(4.3) \quad v_2(N_E) = v_2(N_F) = 6,$$

$$(4.4) \quad v_{\mathfrak{q}_5}(N_E) = 0 \text{ when } 5 \nmid a+b \text{ and } v_{\mathfrak{q}_5}(N_E) = 2 \text{ when } 5 \mid a+b,$$

$$(4.5) \quad v_{\mathfrak{q}_5}(N_F) = 2 \text{ when } 5 \nmid a+b \text{ and } v_{\mathfrak{q}_5}(N_F) = 0 \text{ when } 5 \mid a+b.$$

In [23], the work of Ellenberg on  $\mathbb{Q}$ -curves (see [25, Proposition 3.2]) was used to establish that the mod  $p$  Galois representations attached to  $E$  and  $F$  are irreducible for  $p = 11$  and  $p \geq 17$ . We now improve this conclusion without using the fact that  $E$  and  $F$  are  $\mathbb{Q}$ -curves.

**Proposition 1.** *Let  $d \geq 1$  be an integer such that all its prime factors  $\ell$  satisfy  $\ell \not\equiv 1 \pmod{5}$ . Suppose  $(a, b, c)$  is a primitive solution to (1.2) with  $r = 5$  and  $p \geq 3$ . Then*

- (1)  $\overline{\rho}_{E,p}$  is irreducible if  $5 \nmid a+b$ ,
- (2)  $\overline{\rho}_{F,p}$  is irreducible if  $5 \mid a+b$ .

*Proof.* Let  $p \geq 3$  and put  $C = E$  if  $5 \nmid a+b$ , and  $C = F$  if  $5 \mid a+b$ .

Let us denote by  $\overline{\rho}_{C,p}^{ss}$  the semi-simplification of the representation  $\overline{\rho}_{C,p}$ . Suppose  $\overline{\rho}_{C,p}^{ss} \cong \theta \oplus \theta'$  with the characters  $\theta, \theta'$  satisfying  $\theta\theta' = \chi_p$  where  $\chi_p$  denotes the mod  $p$  cyclotomic character. Since the narrow class group of  $\mathbb{Q}(\sqrt{5})$  is 1 we can write  $\theta = \epsilon\epsilon_p$  and  $\theta' = \epsilon^{-1}\epsilon'_p$ , where  $\epsilon$  is unramified at the primes above  $p$  and  $\epsilon_p, \epsilon'_p$  ramify only at the primes above  $p$ . Furthermore,  $\epsilon$  is unramified outside the bad primes  $\mathfrak{q} \nmid p$  of  $C$ . The additive prime 2 of  $C$  satisfies  $\text{Norm}(2) = 4$  and it follows from  $v_2(N_C) = 6$  and [30, Theorem 1.5] that level lowering at 2 cannot occur. We conclude that the conductor exponent at 2 of  $\epsilon$  is  $v_2(N_C)/2 = 3$  as the conductors of  $\epsilon$  and  $\epsilon^{-1}$  are equal.

Since 2 is the only additive prime of  $C$  (see (4.3)-(4.5) above), we conclude that  $\epsilon$  has conductor  $2^3$ . The Ray class group of  $\mathbb{Q}(\sqrt{5})$  of modulus  $2^3$  together with the two real places is  $(\mathbb{Z}/2\mathbb{Z})^3$ . In particular,  $\theta|_{I_2} = \epsilon|_{I_2}$  is of order 2, where  $I_2 \subset G_{\mathbb{Q}(\sqrt{5})}$  is an inertia subgroup at 2. We conclude that  $\overline{\rho}_{C,p}^{ss}|_{I_2} \cong \theta|_{I_2} \oplus \theta'|_{I_2} = \epsilon|_{I_2} \oplus \epsilon^{-1}|_{I_2}$  has order 2.

Finally, we have  $v_2(j_C) = 6$  hence  $C$  has potentially good reduction at 2 and it follows from part 5 of the Theorem in [17, Section 1] that  $\overline{\rho}_{C,p}(I_2)$  is cyclic of order 4 or isomorphic to the quaternion group. Since the order of inertia is not divisible by  $p$  and we have  $\overline{\rho}_{C,p}|_{I_2} = \overline{\rho}_{C,p}^{ss}|_{I_2}$  which has order 2, a contradiction.

□



The following lemma summarizes Steps 2–4 of the modular method as applied to the Frey curves  $E$  and  $F$ .

**Lemma 2.** *Let  $d \geq 1$  be a integer such that all the prime factors  $\ell$  of  $d$  satisfy  $\ell \not\equiv 1 \pmod{5}$ . Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.2) with  $r = 5$  and  $p \geq 5$ .*

*Write  $E = E_{a,b}$  and  $F = F_{a,b}$ . Then, there exist a Hilbert newform  $f$  over  $\mathbb{Q}(\sqrt{5})$  of parallel weight 2, trivial character and level  $2^6$  and a prime ideal  $\mathfrak{p}$  above  $p$  in the coefficient field of  $f$  such that*

$$\overline{\rho}_{f,\mathfrak{p}} \cong \overline{\rho}_{F,p}, \quad \text{or} \quad \overline{\rho}_{f,\mathfrak{p}} \cong \overline{\rho}_{E,p},$$

*according to whether 5 divides  $a + b$  or not.*

*Proof.* This follows by applying modularity [27] and level lowering for Hilbert modular forms (see [29], [31], [38]), with irreducibility coming from Proposition 1 above, and the determination of Artin conductors from (4.3)–(4.5).  $\square$

**4.3. Bounding the exponent.** Let  $q \neq 2, 5$  be a rational prime such that  $q \not\equiv 1 \pmod{5}$ . Let  $\mathfrak{q}$  be a prime in  $\mathbb{Q}(\sqrt{5})$  above  $q$ . It follows from [26, §2.1] and the discriminants formulas (4.1) and (4.2) that for any integers  $x, y$  with  $(x, y) \neq (0, 0)$  and  $0 \leq x, y \leq q - 1$ , both elliptic curves  $E_{x,y}$  and  $F_{x,y}$  have good reduction at  $\mathfrak{q}$ . Define

$$(4.6) \quad a_{\mathfrak{q}}(E_{x,y}) = \#\mathbb{F}_{\mathfrak{q}} + 1 - \#\widetilde{E}_{x,y}(\mathbb{F}_{\mathfrak{q}}) \quad \text{and} \quad a_{\mathfrak{q}}(F_{x,y}) = \#\mathbb{F}_{\mathfrak{q}} + 1 - \#\widetilde{F}_{x,y}(\mathbb{F}_{\mathfrak{q}})$$

where  $\mathbb{F}_{\mathfrak{q}}$  is the residual field at  $\mathfrak{q}$  and  $\widetilde{E}_{x,y}$  and  $\widetilde{F}_{x,y}$  denote the reductions modulo  $\mathfrak{q}$  of  $E_{x,y}$  and  $F_{x,y}$  respectively.

For any Hilbert newform  $h$  over  $\mathbb{Q}(\sqrt{5})$  of parallel weight 2, trivial character and level  $2^6$ , we define the following integers

$$\mathcal{E}_q(h) = \prod_{\substack{0 \leq x, y \leq q-1 \\ (x,y) \neq (0,0)}} \gcd(\{\text{Norm}(a_{\mathfrak{q}}(E_{x,y}) - a_{\mathfrak{q}}(h)) : \mathfrak{q} \mid q\})$$

and

$$\mathcal{F}_q(h) = \prod_{\substack{0 \leq x, y \leq q-1 \\ (x,y) \neq (0,0)}} \gcd(\{\text{Norm}(a_{\mathfrak{q}}(F_{x,y}) - a_{\mathfrak{q}}(h)) : \mathfrak{q} \mid q\})$$

where  $\mathfrak{q}$  runs through the prime ideals above  $q$  in  $\mathbb{Q}(\sqrt{5})$  and  $a_{\mathfrak{q}}(h)$  denotes the  $\mathfrak{q}$ -th Fourier coefficient of  $h$ .

Let now  $a$  and  $b$  be integers such that  $a^5 + b^5 \neq 0$ . Then for any such ideal  $\mathfrak{q}$  in  $\mathbb{Q}(\sqrt{5})$  dividing  $q$  as above, we have, using (4.6), that  $a_{\mathfrak{q}}(E_{a,b}) = a_{\mathfrak{q}}(E_{x,y})$  where  $(x, y) \in \{0, \dots, q-1\}^2 \setminus \{(0, 0)\}$  are defined by  $(a, b) \equiv (x, y) \pmod{q}$ .

**Proposition 2.** *Let  $d \geq 1$  be an integer such that all its prime factors  $\ell$  satisfy  $\ell \not\equiv 1 \pmod{5}$ . Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.2) with  $r = 5$  and  $p \geq 5$ .*

*Then, there exists a Hilbert newform  $f$  over  $\mathbb{Q}(\sqrt{5})$  of parallel weight 2, trivial character and level  $2^6$  such that for any prime  $q \neq 2, 5$  with  $q \not\equiv 1 \pmod{5}$ , we have  $p \mid q\mathcal{E}_q(f)$  or  $p \mid q\mathcal{F}_q(f)$  respectively if  $5 \nmid a + b$  or  $5 \mid a + b$ .*

*Proof.* This follows from Lemma 2 and our definitions.  $\square$

The following summarizes part of Step 5 of the modular method as applied to Frey curves  $E$  and  $F$ .

**Proposition 3.** *Let  $d \geq 1$  be an integer such that all its prime factors  $\ell$  satisfy  $\ell \not\equiv 1 \pmod{5}$ . Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.2) with  $r = 5$ .*

- (1) *If  $5 \nmid a + b$  and  $p \geq 7$  then  $\overline{\rho}_{E,p}$  is isomorphic to the mod  $p$  representation of one of the curves*

$$E_{1,0}, \quad E_{1,0} \otimes \chi_{-1}, \quad E_{1,0} \otimes \chi_2, \quad E_{1,0} \otimes \chi_{-2}, \quad E_{1,1}, \quad E_{1,1} \otimes \chi_2;$$

- (2) *If  $5 \mid a + b$  and  $p \geq 11$  then  $\overline{\rho}_{F,p}$  is isomorphic to the mod  $p$  representation of one of the curves*

$$F_{1,-1} \quad \text{or} \quad F_{1,-1} \otimes \chi_2,$$

where  $\chi_D$  denotes the quadratic character corresponding to the field  $\mathbb{Q}(\sqrt{D})$ .

*Proof.* Using [6], we do the following: we compute all the newforms over  $\mathbb{Q}(\sqrt{5})$  of level  $2^6$ , parallel weight 2 and trivial character. For each such newform  $h$ , we compute  $q\mathcal{E}_q(h)$  and  $q\mathcal{F}_q(h)$  for all prime  $q \leq 30$  as above.

Suppose  $5 \nmid a + b$ . From the previous proposition it follows that, for each  $h$ , if  $p$  does not divide the gcd of all  $q\mathcal{E}_q(h)$  we can discard  $h$  for that  $p$ . This allows to discard all except 6 newforms for  $p \geq 7$  (we note that  $p \geq 5$  works for all except two newforms); we identify the remaining 6 newforms with twists of the Frey curves  $E_{1,0}$  and  $E_{1,1}$ .

Suppose  $5 \mid a + b$ . From the previous proposition it follow that, for each  $h$ , if  $p$  does not divide the gcd of all  $q\mathcal{F}_q(h)$  we can discard  $h$  for that  $p$ . This allows to discard all except 2 newforms for  $p \geq 11$ ; the remaining 2 newforms correspond to  $F_{1,-1}$  and its quadratic twist by 2.  $\square$

**4.4. Proof of Theorem 1.** Let  $(a, b, c)$  be a putative non-trivial primitive solution to equation (1.3).

The cases  $p = 2$ ,  $p = 3$  and  $p = 5$  follow from [2, Theorem 1.1], [4, Theorem 1.5] and [24, Théorème IX] respectively. Hence we can assume  $p \geq 7$ .

It follows from [23, Lemma 2.2] that  $3 \mid a + b$ . This imposes a very strong restriction on the value of the trace of Frobenius of  $E_{a,b}$  at the unique prime ideal  $\mathfrak{q}$  above 3 in  $\mathbb{Q}(\sqrt{5})$ . Namely, the elliptic curve  $E_{a,b}$  reduces modulo  $\mathfrak{q}$  to the curve defined by  $y^2 = x^3 - \bar{\omega}^2 x$ . Hence, we have  $a_{\mathfrak{q}}(E_{a,b}) = 6$ .

Note that the elliptic curves  $E_{x,y}$  that appear in part (1) of Proposition 3 satisfy  $x + y \not\equiv 0 \pmod{3}$ . Therefore, one may hope to discard them by computing their trace of Frobenius at  $\mathfrak{q}$ . Indeed, we find that the  $a_{\mathfrak{q}}$  coefficient of the curves  $E_{1,0}$ ,  $E_{1,0} \otimes \chi_{-1}$ ,  $E_{1,0} \otimes \chi_2$ ,  $E_{1,0} \otimes \chi_{-2}$ ,  $E_{1,1}$ , and  $E_{1,1} \otimes \chi_2$  is 4. We have thus proved the following result.

**Proposition 4.** *Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.3) for  $p \geq 7$ .*

*Then 5 divides  $a + b$ . Furthermore, if  $p \geq 11$ , then  $\overline{\rho}_{F,p}$  is isomorphic to the mod  $p$  representation of one of the curves  $F_{1,-1}$  or  $F_{1,-1} \otimes \chi_2$ .*

*In particular, (1.3) has no non-trivial primitive solutions satisfying  $5 \nmid a + b$  for  $p \geq 7$ .*

*Remark 4.7.* The previous type of argument does not always work; for instance, when  $r = 7$  and  $d = 3$  in equation (1.2), the condition  $3 \mid a + b$  does not distinguish  $E_{(0,1)}$  and  $E_{(1,-1)}$  by traces of Frobenius at 3, where  $E_{(a,b)}$  is the Frey curve in last paragraph of [26, p. 630].

So far, our approach to Theorem 1 in the case  $p \geq 7$  only uses the Frey curves  $E$  and  $F$ . We now take into account the information coming from the rational Frey curve  $W = W_{a,b}$  introduced in Section 4.1.

The case  $p = 7$  of equation (1.3) is dealt with explicitly in [5, pp. 186-190] by applying the so-called reduction method of Kraus to  $W$ . We therefore assume  $p \geq 11$ .

From Lemma 1 we can further assume that  $v_2(a) = 1$ . Write

$$F = F_{a,b}, \quad C = F_{1,-1}, \quad C' = F_{1,-1} \otimes \chi_2.$$

From Proposition 4 we know that

$$\bar{\rho}_{F,p} \cong \bar{\rho}_{C,p} \quad \text{or} \quad \bar{\rho}_{F,p} \cong \bar{\rho}_{C',p}.$$

Recall that 2 is inert in  $\mathbb{Q}(\sqrt{5})$  and  $I_2$  denotes an inertia subgroup. We will now show the isomorphisms above do not hold by applying version 1 of the image of the inertia argument at 2 (see Section 3).

The model for the Frey curve  $F$  has the following standard invariants

$$(4.8) \quad c_4(F) = 2^4 \left( 4(a-b)^2 - 3 \left( \frac{-3(\omega - \bar{\omega})}{10} + \frac{1}{2} \right) \psi_5(a, b) \right)$$

$$(4.9) \quad c_6(F) = -2^6(a-b) \left( 8(a-b)^2 - 9 \left( \frac{-3(\omega - \bar{\omega})}{10} + \frac{1}{2} \right) \psi_5(a, b) \right)$$

$$(4.10) \quad \Delta(F) = 2^6 \left( \frac{-3}{10}(\omega - \bar{\omega}) + \frac{1}{2} \right)^2 \left( \frac{3}{10}(\omega - \bar{\omega}) + \frac{1}{2} \right) \phi_5(a, b) \psi_5(a, b).$$

Since  $v_2(a) = 1$  we have  $v_2(b) = 0$  and it follows that

$$v_2(c_4(F)) = 4, \quad v_2(c_6(F)) = 6, \quad v_2(\Delta(F)) = 6;$$

furthermore, the model is minimal and  $v_2(j(F)) = 6$ . From the corollary in [17, Section 1] we see that  $\bar{\rho}_{F,p}(I_2)$  has order 8.

Specializing the above formulas at  $(a, b) = (1, -1)$  gives the following valuations for the standard invariants of  $C$  :

$$v_2(c_4(C)) = 4, \quad v_2(c_6(C)) = 7, \quad v_2(\Delta(C)) = 10, \quad v_2(j(C)) = 6.$$

The elliptic curve  $C'$  has equation

$$y^2 = x^3 + 8x^2 + (-4(\omega - \bar{\omega}) + 8)x$$

and we compute the valuations at 2 of its standard invariants as above :

$$v_2(c_4(C')) = 6, \quad v_2(c_6(C')) = 10, \quad v_2(\Delta(C')) = 12, \quad v_2(j(C')) = 6.$$

Let us put

$$c'_4(C) = \frac{c_4(C)}{2^4} \quad \text{and} \quad c'_4(C') = \frac{c_4(C')}{2^6}.$$

One checks that we have  $c'_4(C) = c'_4(C') = 3(\omega - \bar{\omega}) + 10$ . Moreover, one has

$$v_2(3(\omega - \bar{\omega}) + 10 - 1) = 1 \quad \text{and} \quad v_2((3(\omega - \bar{\omega}) + 10 - 1)/2 - 1) = 0.$$

Therefore,  $3(\omega - \bar{\omega}) + 10 \equiv j(j^2 + 2) \pmod{4}$  where  $j \in \mathbb{Q}_2(\sqrt{5})$  is a primitive cube root of unity. According to the item (c.1) of the corollary in [17, Section 1], it follows that  $\bar{\rho}_{C,p}(I_2)$  and  $\bar{\rho}_{C',p}(I_2)$  are of order 4. This gives the desired contradiction, completing the proof of Theorem 1.

*Remark 4.11.* Note we cannot improve on the result in [23] for  $r = 5$  and  $d = 2$  since we do not have the condition  $3 \mid a + b$  to eliminate the curves in Proposition 3 (1); furthermore, the additional use of the Frey curve  $W_{a,b}$  also does not help because  $W_{1,1}$  is an elliptic curve without complex multiplication.

## 5. PARTIAL RESULTS FOR $x^5 + y^5 = dz^p$ WITH $d = 1, 2$

It is sometimes possible to resolve equation (1.2) by assuming additional  $q$ -adic conditions to avoid the obstructing trivial solutions. In this section we provide such examples regarding the equation

$$(5.1) \quad x^5 + y^5 = dz^p, \quad \text{where} \quad d \in \{1, 2\}.$$

First note that the conditions on  $c$  of Theorem 4 can easily be translated into divisibility conditions on  $a + b$ . More precisely, Theorem 4 follows from the following two theorems.

**Theorem 5.** *Assume  $d = 1, 2$ . Then, for all primes  $p$ , there are no non-trivial primitive solutions  $(a, b, c)$  to (5.1) satisfying  $5 \mid a + b$ .*

**Theorem 6.** *Assume  $d = 1$  (resp.  $d = 2$ ). Then, for all primes  $p$ , there are no non-trivial primitive solutions to (5.1) satisfying  $2 \mid a + b$  (resp.  $4 \mid a + b$ ).*

We want to emphasize that, in the proof of Theorem 5, using the multi-Frey technique we are able to force a Frey curve to have multiplicative reduction at 3.

These results, and their proofs, should illustrate clearly to the reader that the obstruction to solving (5.1) with  $d = 1$  (resp.  $d = 2$ ) is that none of the Frey curves we use are sensitive to the trivial solutions  $\pm(1, 0, 1), \pm(0, 1, 1)$  (resp.  $\pm(1, 1, 1)$ ).

**5.1. Proof of Theorem 5.** The cases  $p = 2$  and  $p = 3$  follow from [2, Theorem 1.1], [4, Theorem 1.5], respectively. It follows from Fermat's Last Theorem and the main theorem of [20] that the result holds for  $p = 5$ . Hence we can assume  $p \geq 7$ .

Let  $(a, b, c)$  be a putative non-trivial primitive solution to equation (5.1) with  $d = 1, 2$ , exponent  $p \geq 7$  and  $5 \mid a + b$ .

By part (2) of Proposition 3 we have  $\bar{\rho}_{F,p} \cong \bar{\rho}_{A,p}$ , where  $A = F_{1,-1}$  or  $F_{1,-1} \otimes \chi_2$  when  $p \geq 11$ ; furthermore, from its proof it follows that for  $p = 7$  we can have  $\bar{\rho}_{F,p} \cong \bar{\rho}_{A,p}$  or  $\bar{\rho}_{F,p} \cong \bar{\rho}_{f,p}$ , where  $f$  is one of other 3 possible newforms.

The traces of Frobenius at 3 of these five newforms satisfy  $a_3(A) = a_3(f) = 4$ ; using [6] to compute  $a_3(F_{a,b})$  shows that  $3 \mid a + b$  (if not, then  $a_3(F_{a,b}) \neq a_3(A)$  and we get that  $p \mid 6$ , which is not the case). This means the curve  $W = W_{a,b}$  from Section 4.1 has multiplicative

reduction at 3 (see for instance, proof of [5, Lemme 2.7]). Note that this is another instance of using the multi-Frey technique.

From [5, Proposition 3.1] we have that  $\bar{\rho}_{W,p}$  is irreducible for  $p \geq 7$ . A standard application of the modular method with  $W$  (which follows Propositions 3.3 and 3.4 of *loc. cit.*) gives that  $\bar{\rho}_{W,p} \cong \bar{\rho}_{f,p}$ , where  $f$  is a rational newform of weight 2, trivial Nebentypus and level  $2^4 \cdot 5^2$ ,  $2^3 \cdot 5^2$ , or  $2 \cdot 5^2$  for  $d = 1$  and  $v2^4 \cdot 5^2, 2 \cdot 5^2$  for  $d = 2$ . Now, since level lowering is happening at the prime 3, we must have that  $p \mid (3+1)^2 - a_3(f)^2$ .

A computation then shows that  $p \in \{2, 3, 5, 7\}$ , yielding a contradiction with  $p \geq 11$ .

Furthermore, the exponent  $p = 7$  in the list above is due to four newforms  $f$  all satisfying  $\#\bar{\rho}_{f,7}(I_5) = 3$  or 6, where  $I_5$  is an inertia subgroup at 5. On the other hand,  $W$  has potentially multiplicative reduction at 5 (since  $5 \mid a+b$ ) hence  $\#\bar{\rho}_{W,7}(I_5) = 2$  or 14, giving a contradiction also for  $p = 7$ .

**5.2. Proof of Theorem 6.** As in the previous proof, the result is known for  $p \leq 5$ . Let  $(a, b, c)$  be a putative non-trivial primitive solution to equation (5.1) with  $d = 1$  and  $2 \mid a+b$  (resp.  $d = 2$  and  $4 \mid a+b$ ) for  $p \geq 7$ .

In the case  $d = 1$ , the condition  $2 \mid a+b$  implies that in fact  $8 \mid a+b$ , because  $2 \mid c$ ,  $p \geq 7$  and  $2 \nmid \phi_5(a, b)$ , where we recall  $a^5 + b^5 = (a+b)\phi_5(a, b) = dc^p$ ; in the case  $d = 2$ , the condition  $4 \mid a+b$  also implies that in fact  $8 \mid a+b$ . So we now assume  $8 \mid a+b$ .

By Theorem 5, we may assume  $5 \nmid a+b$ , and then invoking part (1) of Proposition 3 we deduce  $\bar{\rho}_{E,p} \cong \bar{\rho}_{A,p}$  where  $A = E_{1,0}, E_{1,0} \otimes \chi_{-1}, E_{1,0} \otimes \chi_2, E_{1,0} \otimes \chi_{-2}, E_{1,1},$  or  $E_{1,1} \otimes \chi_2$ .

The result now follows from version 2 of the image of inertia argument (see Section 3). Indeed, from  $\bar{\rho}_{E,p} \cong \bar{\rho}_{A,p}$  we know that the inertial field at 2 of  $E$  and  $A$  must be the same. By Proposition 5 below and the assumption  $8 \mid a+b$ , we see this is not possible, as desired.

Write  $L_{a,b} = L_{E_{a,b}}$  for the inertial field at 2 corresponding to the Frey curve  $E_{a,b}$  (i.e. the field fixed by the kernel of  $\bar{\rho}_{E_{a,b},m}(I_2)$  for any  $m \geq 3$  coprime to 2). Respectively, for  $x, y \in \mathbb{Z}$  such that  $x^5 + y^5 \neq 0$ , we write  $L_{x,y,D}$  for the inertial field at 2 corresponding to the curve  $E_{x,y} \otimes \chi_D$ .

**Proposition 5.** *Suppose  $(a, b, c)$  is a non-trivial primitive solution to (5.1) satisfying  $8 \mid a+b$ . Then  $L_{a,b} \neq L_{1,0}, L_{1,0,-1}, L_{1,0,2}, L_{1,0,-2}, L_{1,1}, L_{1,1,2}$ .*

*Proof.* This is verified using [6] by considering a subfield  $M$  of the 3-division field of  $A$  over  $F$  with the property that  $A$  has good reduction at a prime above 2 of  $M$ , but  $E_{a,b}$  does not have good reduction at this prime above 2 of  $M$  if  $8 \mid a+b$ . We take  $M$  to be the subfield generated by the  $x$  and  $y$  coordinates of a choice of 3-torsion point of  $A$ .

In the case where  $A = E_{1,1}, E_{1,1} \otimes \chi_2$ , the choice of  $M$  has degree 4 over  $\mathbb{Q}(\sqrt{5})$ , whereas the full 3-division field of  $A$  has degree 8 over  $\mathbb{Q}(\sqrt{5})$ .

In the case where  $A = E_{1,0}, E_{1,0} \otimes \chi_{-1}, E_{1,0} \otimes \chi_2, E_{1,0} \otimes \chi_{-2}$ , the choice of  $M$  has degree 8 over  $\mathbb{Q}(\sqrt{5})$ , whereas the full 3-division field of  $A$  has degree 48 over  $\mathbb{Q}(\sqrt{5})$ .  $\square$

## 6. A RESULT ON THE SECOND CASE

In this section, we prove Theorem 3. The following proposition is known to experts, but we have not been able to find a suitable reference for it, so we include a proof.

**Proposition 6.** *Let  $f$  be a newform of weight 2, trivial character and level  $N$ . Let  $p$  be an odd prime not dividing  $N$ , and let  $a_p$  denote the  $p$ -th Fourier coefficient of  $f$ . Then, a necessary condition for the existence of a congruence between the  $p$ -adic Galois representation attached to  $f$  and the one attached to a newform  $g$  of level  $pN$ , trivial character and weight 2 is :*

$$a_p \equiv \pm 1 \pmod{p}.$$

*Proof.* Denote by  $\rho_{f,p}$  and  $\rho_{g,p}$  the restrictions to  $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$  of the respective global  $p$ -adic Galois representations attached to  $f$  and  $g$ . Then  $f$  congruent to  $g$  modulo  $p$  implies in particular that the semi-simplifications of the residual local representations  $\bar{\rho}_{f,p}^{ss}$  and  $\bar{\rho}_{g,p}^{ss}$  of, respectively,  $\rho_{f,p}$  and  $\rho_{g,p}$  are isomorphic. We assume  $p > 2$ . Since  $\rho_{g,p}$  is semistable non-crystalline of weight 2,  $\bar{\rho}_{g,p}^{ss}$  is reducible and isomorphic to:  $\chi_p \text{unr}(\mu) \oplus \text{unr}(\mu)$  for some mod  $p$  unit  $\mu$  and where  $\chi_p$  denotes the mod  $p$  cyclotomic character (this is the case  $k = 2$  of [10, Théorème 1.2]). Thus, the same holds for  $\bar{\rho}_{f,p}^{ss}$ . By [9, Théorème 6.7] (a theorem that puts together results of Deligne, Serre, Fontaine and Edixhoven) this forces  $a_p$  to be congruent to  $\pm 1$  modulo  $p$ .  $\square$

Using the above proposition, we now prove Theorem 3.

The cases  $p = 2$  and  $p = 3$  follow from [2, Theorem 1.1], [4, Theorem 1.5], respectively. It follows from Fermat's Last Theorem and the main theorem of [20] that the result holds for  $p = 5$ . Hence we can assume  $p \geq 7$ .

We know (see [5, Proposition 3.1]) that the mod  $p$  Galois representation attached to the Frey curve  $W$  is irreducible, for every  $p \geq 7$ . By level lowering, we have a congruence modulo  $p$  between the Frey curve  $W$  and some weight 2 newform of level  $N = 50, 200$  or  $400$ . Since we are assuming that  $p$  divides  $c$ , level raising at  $p$  mod  $p$  is happening for this specific newform. This implies in particular that the necessary condition in Proposition 6 must hold.

All newforms in these spaces correspond to (isogeny classes of) elliptic curves over  $\mathbb{Q}$ , and we consider the cases when:

- (1) the elliptic curve does not have a rational 2-torsion point, or
- (2) the elliptic curve has a rational 2-torsion point.

Case (1): For all such elliptic curves, it can be checked [6] that the coefficient  $a_3$  equals  $\pm 1$  or  $\pm 3$ . Then we easily conclude using the congruence between these values and  $0, \pm 2, \pm 4$  that this can not happen for  $p > 7$ . We are using the fact that the Frey curve  $W$  has a rational 2-torsion point, and we are covering both the cases of  $W$  having good or multiplicative reduction at 3. For  $p = 7$ , the congruence forces  $a_3 = \pm 3$ . We then quickly check that none of the curves of level  $N \in \{50, 200, 400\}$  satisfies both  $a_3 = \pm 3$  and  $a_7 \equiv \pm 1 \pmod{7}$ .

Case (2): The fact that mod  $p$  we have level raising at  $p$  forces the necessary condition in Proposition 6 to hold:  $a_p \equiv \pm 1 \pmod{p}$ , which, for an elliptic curve, implies  $a_p = \pm 1$  by



the Hasse bound. But all curves in case (2) have a rational 2-torsion point, thus all their coefficients  $a_q$  for  $q \nmid N$  are even. This gives a contradiction.

## 7. A MULTI-FREY APPROACH TO THE EQUATION $x^{13} + y^{13} = 3z^p$

In this section, we will use the following factorization and notation

$$(7.1) \quad x^{13} + y^{13} = (x + y)\phi_{13}(x, y) = (x + y)\psi_{13}(x, y)\bar{\psi}_{13}(x, y),$$

where

$$(7.2) \quad \psi_{13}(x, y) = x^6 + \frac{1}{2}(w - 1)x^5y + 2x^4y^2 + \frac{1}{2}(w + 1)x^3y^3 + 2x^2y^4 + \frac{1}{2}(w - 1)xy^5 + y^6,$$

and  $\bar{\psi}_{13}(x, y)$  are the two degree 6 irreducible factors of  $\phi_{13}(x, y)$  over  $\mathbb{Q}(\sqrt{13})$ , where  $w \in \mathbb{Q}(\sqrt{13})$  satisfies  $w^2 = 13$ .

**7.1. The modular method over  $\mathbb{Q}(\sqrt{13})$ .** We will now prove the following theorem by sharpening the methods in [22] plus a refined image of inertia argument.

**Theorem 7.** *Let  $p \geq 5$ ,  $p \neq 13$  be a prime. Then,*

- (A) *the equation (1.4) has no non-trivial primitive solutions  $(a, b, c)$  such that  $13 \nmid c$ ;*
- (B) *the equation (1.4) has no non-trivial primitive solutions  $(a, b, c)$  such that  $4 \nmid a + b$ .*

Before entering the proof of the theorem, we first introduce tools from [22] which are valid beyond the case  $d = 3$  of equation (1.4). Suppose that  $(a, b, c)$  is a primitive solution to (1.2) with  $r = 13$ . We attach to  $(a, b, c)$  the Frey elliptic curve  $E_{(a,b)}$  defined over  $\mathbb{Q}(\sqrt{13})$  by the model

$$E_{(a,b)} : y^2 = x^3 + a_4(a, b)x + a_6(a, b),$$

where

$$\begin{aligned} a_4(a, b) &= (216w - 2808)a^4 + (-1728w + 5616)a^3b \\ &\quad + (1728w - 11232)a^2b^2 + (-1728w + 5616)ab^3 \\ &\quad + (216w - 2808)b^4, \\ a_6(a, b) &= (-8640w + 44928)a^6 + (49248w - 235872)a^5b \\ &\quad + (-129600w + 471744)a^4b^2 + (152928w - 662688)a^3b^3 \\ &\quad + (-129600w + 471744)a^2b^4 + (49248w - 235872)ab^5 \\ &\quad + (-8640w + 44928)b^6. \end{aligned}$$

The discriminant of  $E_{(a,b)}$  is then given by the following formula :

$$\Delta(E_{(a,b)}) = 2^{16} \cdot 3^{12} \cdot 13 \cdot \psi_{13}(a, b)^2.$$

The next proposition gives us the required irreducibility of the mod  $p$  representation of  $E = E_{(a,b)}$ .

**Proposition 7.** *Let  $d \geq 1$  be an integer such that all its prime factors  $\ell$  satisfy  $\ell \not\equiv 1 \pmod{13}$ . Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.2) with  $r = 13$  and  $p \geq 7$ . Then the Galois representation  $\bar{\rho}_{E,p}$  is irreducible.*

*If in addition we have that  $3 \mid d$ , then  $\bar{\rho}_{E,5}$  is also irreducible.*

*Proof.* We note that the proof of [28, Theorem 3] does not depend on the value of  $d$  in *loc.cit*, therefore it proves the proposition for  $p = 11$  and  $p \geq 17$ . Assume therefore that  $p \in \{5, 7, 13\}$ .

We note that 3 splits in  $\mathbb{Q}(\sqrt{13})$  and let  $\mathfrak{q}_1, \mathfrak{q}_2$  be the primes above it with  $w + 1 \in \mathfrak{q}_1$  (and  $w - 1 \in \mathfrak{q}_2$ ). The primes  $\mathfrak{q}_1$  and  $\mathfrak{q}_2$  are primes of good reduction of  $E$ ; since  $a, b \in \mathbb{Z}$  we can check that the pairs of traces of Frobenius at these primes  $(a_{\mathfrak{q}_1}(E), a_{\mathfrak{q}_2}(E))$  satisfy

$$(a_{\mathfrak{q}_1}(E), a_{\mathfrak{q}_2}(E)) \in \{(-3, -1), (-1, -3), (-1, 1)\}.$$

Moreover, the case  $(-3, -1)$  occurs precisely when  $3 \mid a + b$ . Therefore, we can compute the corresponding pairs of characteristic polynomials of  $(\bar{\rho}_{E,p}(\text{Frob}_{\mathfrak{q}_1}), \bar{\rho}_{E,p}(\text{Frob}_{\mathfrak{q}_2}))$  which are given by

$$(7.3) \quad (x^2 - a_{\mathfrak{q}_1}(E)x + 3, x^2 - a_{\mathfrak{q}_2}(E)x + 3).$$

Now suppose that  $\bar{\rho}_{E,p}$  is reducible. Then, for any prime  $\mathfrak{q}$  in  $\mathbb{Q}(\sqrt{13})$  of good reduction of  $E$ , the characteristic polynomial of  $\bar{\rho}_{E,p}(\text{Frob}_{\mathfrak{q}})$  must factor over  $\mathbb{F}_p$  into two linear polynomials. In particular, this holds for  $\mathfrak{q} = \mathfrak{q}_1, \mathfrak{q}_2$ .

We check that for  $p = 5, 7$ , and  $13$ , that each of the pairs of polynomials in (7.3) always contains one polynomial that does not factor over  $\mathbb{F}_p$  except when  $p = 5$  and  $(a_{\mathfrak{q}_1}(E), a_{\mathfrak{q}_2}(E)) = (-1, 1)$ . This proves the proposition for  $p \geq 7$ . Finally, assume  $3 \mid d$  and  $p = 5$ ; hence  $3 \mid a + b$  and we already observed that  $(a_{\mathfrak{q}_1}(E), a_{\mathfrak{q}_2}(E)) = (-3, -1) \neq (-1, 1)$ . We conclude  $\bar{\rho}_{E,5}$  is irreducible, finishing the proof.  $\square$

The following lemma summarizes Steps 2–4 of the modular method as applied to the Frey curve  $E$ .

**Lemma 3.** *Let  $d \geq 1$  be an integer such that all its prime factors  $\ell$  satisfy  $\ell \not\equiv 1 \pmod{13}$ . Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.2) with  $r = 13$  and  $p \geq 7$ . Write  $E = E_{(a,b)}$ . Then,*

$$(7.4) \quad \bar{\rho}_{E,p} \cong \bar{\rho}_{f,p},$$

where  $f$  is an Hilbert newform over  $\mathbb{Q}(\sqrt{13})$  of parallel weight 2, trivial character and level

$$N_f = 2^s w^2, \quad \text{where } s = 3, 4.$$

Moreover, when  $a + b$  is even,  $s = 3$  if  $4 \mid a + b$  and  $s = 4$  if  $4 \nmid a + b$ .

If in addition we have that  $3 \mid d$ , then the above also holds for  $\bar{\rho}_{E,5}$ .

*Proof.* This follows from modularity [27], Tate's algorithm (see [22, Proposition 3.3]) and level lowering for Hilbert modular forms (see [29], [31], [38]).  $\square$

**Proposition 8.** *Let  $d \geq 1$  be an integer such that all its prime factors  $\ell$  satisfy  $\ell \not\equiv 1 \pmod{13}$ . Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.2) with  $r = 13$  and  $p \geq 7$ ,  $p \neq 13$ . Write  $E = E_{(a,b)}$ . Then,*

$$(7.5) \quad \bar{\rho}_{E,p} \cong \bar{\rho}_{Z,p},$$

where  $Z$  is one of the following elliptic curves

$$E_{(1,-1)}, \quad E_{(1,0)} \quad \text{or} \quad E_{(1,1)}.$$

If in addition we have that  $3 \mid d$ , then we also have  $\bar{\rho}_{E,5} \cong \bar{\rho}_{Z,5}$  for  $Z$  as above.

*Proof.* Using [6], we compute the Hilbert newforms given by the previous lemma and we apply the same method as in Section 4.3 to bound the exponent  $p$ . More precisely, for  $p \geq 5$ ,  $p \neq 13$  we eliminate all the forms except for those corresponding to the three elliptic curves in the statement and another form  $g$  which cannot be eliminated for  $p = 7$ . This form  $g$  has level  $2^3 w^2$ , field of coefficients  $\mathbb{Q}(\sqrt{2})$  and cannot be eliminated for the exponent  $p = 7$ , even using ‘many’ auxiliary primes  $q \neq 2, 13$ .

We deal with  $g$  and  $p = 7$  by treating the two primes  $\mathfrak{q}_1, \mathfrak{q}_2$  above 7 in  $\mathbb{Q}(\sqrt{2})$  separately. Indeed, by comparing traces of Frobenius mod  $\mathfrak{q}_2$  we promptly check that  $\bar{\rho}_{E,7} \not\cong \bar{\rho}_{g,\mathfrak{q}_2}$ ; for the prime  $\mathfrak{q}_1$  comparing enough traces implies  $\bar{\rho}_{g,\mathfrak{q}_1} \cong \bar{\rho}_{E_{(1,-1)},7}$ , as desired.

Under the assumption  $3 \mid d$  the previous lemma applies for  $p = 5$  and, since the computations of this proof also, the last statement follows.  $\square$

*Remark 7.6.* We note that the argument in the previous proof dealing with the form  $g$  and the prime  $\mathfrak{q}_1 \mid 7$  is not completely precise; indeed, we compared traces of Frobenius at primes  $q$  in  $\mathbb{Q}(\sqrt{13})$  of norm up to 5000 and always obtained  $a_q(g) \equiv a_q(E_{(1,-1)}) \pmod{\mathfrak{q}_1}$ . This seems to indicate that  $\bar{\rho}_{g,\mathfrak{q}_1} \cong \bar{\rho}_{E_{(1,-1)},7}$  as used in the proof, but to actually have this conclusion we need to compare traces up to a ‘Sturm bound’ as in [16]. We are working on making this argument fully rigorous.

*Proof of Theorem 7.* Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.4) with  $p \geq 5$  and  $p \neq 13$ . Write  $E = E_{(a,b)}$ . From Proposition 8, we know that  $\bar{\rho}_{E,p} \cong \bar{\rho}_{Z,p}$ , where  $Z$  is  $E_{(1,-1)}$ ,  $E_{(1,0)}$  or  $E_{(1,1)}$ .

Let  $\mathfrak{q}_1$  and  $\mathfrak{q}_2$  be the primes in  $\mathbb{Q}(\sqrt{13})$  dividing 3. Both  $\mathfrak{q}_i$  are primes of good reduction for  $E$  and  $W$ ; since  $3 \mid a + b$  we have that

$$a_{\mathfrak{q}_1}(E) = -3, \quad \text{and} \quad a_{\mathfrak{q}_2}(E) = -1.$$

On the other hand,

$$a_{\mathfrak{q}_1}(E_{(1,0)}) = -1, \quad a_{\mathfrak{q}_2}(E_{(1,0)}) = -3, \quad a_{\mathfrak{q}_1}(E_{(1,1)}) = -1, \quad a_{\mathfrak{q}_2}(E_{(1,1)}) = 1,$$

therefore for  $p \geq 3$  we have  $a_{\mathfrak{q}_i}(E) \not\equiv a_{\mathfrak{q}_i}(Z) \pmod{\mathfrak{p}}$ , hence for  $Z = E_{(1,0)}$  or  $Z = E_{(1,1)}$  we have  $\bar{\rho}_{E,p} \not\cong \bar{\rho}_{Z,p}$ . We conclude that  $Z = E_{(1,-1)}$ .

We now prove (A). Let  $K^+$  be the maximal totally real subfield of  $\mathbb{Q}(\zeta_{13})$  and  $\pi$  denote the prime ideal in  $K^+$  above 13. From [22, Proposition 3.1], when  $13 \nmid a + b$  (or equivalently  $13 \nmid c$ ), the curve  $Z/K^+$  has good reduction at  $\pi$  and  $E/K^+$  has bad additive reduction. The conclusion follows from version 2 of image of inertia argument.

We now prove (B). Consider the base change of  $E_{(a,b)}$  to the field  $M$ , where  $M = \mathbb{Q}(\sqrt{13})(x, y)$ , and  $(x, y)$  is a choice of 3-torsion point of  $Z = E_{(1,-1)}$ . Assuming  $4 \nmid a + b$  and using [6], we check that  $E_{a,b}/M$  has conductor exponent  $\geq 4$ , whereas  $Z/M$  has conductor exponent 2. The conclusion follows from version 3 of the image of inertia argument. We note the full 3-division field of  $Z$  has degree 48 over  $\mathbb{Q}(\sqrt{13})$ , whereas our choice of  $M$  has degree 8 over  $\mathbb{Q}(\sqrt{13})$ , making the computation faster.  $\square$

**7.2. The modular method over the real cubic subfield of  $\mathbb{Q}(\zeta_{13})$ .** In [26], several Frey curves are attached to equation (1.2). In particular, for  $r = 13$  one of them is  $E_{(a,b)}$  from the previous section; in this section we will use another Frey curve from *loc. cit.* defined over a cubic field.

Let  $K^+$  be the maximal (degree 6) totally real subfield of  $\mathbb{Q}(\zeta_{13})$  and write  $K$  for its cubic subfield. Write  $\zeta = \zeta_{13}$  and define

$$A_{x,y} = \alpha(x+y)^2, \quad B_{x,y} = \beta(x^2 + (\zeta + \zeta^{-1})xy + y^2), \quad C_{x,y} = \gamma(x^2 + (\zeta^8 + \zeta^{-8})xy + y^2),$$

where

$$\alpha = \zeta^8 + \zeta^{-8} - \zeta - \zeta^{-1}, \quad \beta = 2 - \zeta^8 - \zeta^{-8}, \quad \gamma = \zeta + \zeta^{-1} - 2.$$

We note that  $A_{x,y}, B_{x,y}, C_{x,y}$  are polynomials in  $K^+$  satisfying  $A_{x,y} + B_{x,y} + C_{x,y} = 0$ .

Let  $(a, b, c)$  be a primitive solution to (1.4) and attach to it the Frey elliptic curve (this curve corresponds to the curve defined by equation (13) with  $(k_1, k_2) = (1, 5)$  in [26])

$$F_{a,b} : y^2 = x(x - A_{a,b})(x + B_{a,b}), \quad \Delta(F_{a,b}) = 2^4(A_{a,b}B_{a,b}C_{a,b})^2,$$

whose short Weierstrass model is defined over  $K$  (see the last paragraph of page 621 of [26]).

Let  $\mathfrak{p}_3$  and  $\mathfrak{p}_{13}$  be the primes of  $K$  above 3 and 13, respectively.

The elliptic curve  $F_{a,b}$  is semistable outside the primes above 2 and 13 by [26, Proposition 4.1] (the proposition cited is for the field  $K^+$ , but  $K^+/K$  is unramified outside  $\mathfrak{p}_{13}$ ). Using [6], we can compute the conductor exponents at the prime above 2 and 13, which shows that the conductor of  $F_{a,b}$  is given by

$$(7.7) \quad N_{F_{a,b}} = 2^s \mathfrak{p}_{13}^2 \mathfrak{p}_3 c', \quad \text{where } s \in \{0, 1, 3, 4\},$$

and  $c'$  is a product of multiplicative primes coprime to  $2 \cdot 3 \cdot 13$ . Furthermore, if  $4 \nmid a+b$  then  $s = 3, 4$  and if  $4 \mid a+b$  then  $s = 0, 1$ .

In particular, we know that  $F_{a,b}$  is semistable at all primes  $v \mid 3$  in  $K$ . Thus, from [26, Theorem 6.3], it follows that  $F_{a,b}$  is modular.

Write  $E = E_{a,b}$  and  $F = F_{a,b}$ . The following illustrates a fundamental difference between the Frey curves  $E$  and  $F$ . Note that irreducibility of  $\bar{\rho}_{E,p}$  followed by an application of [28, Theorem 3] which makes crucial use of the presence of an explicit prime of good reduction of  $E$ . This was guaranteed by the fact that all the primes not dividing  $2 \cdot 13$  of bad reduction of  $E$  must be non-congruent to 1 mod 13 (see formula for  $\Delta(E)$ ); this is no longer the case for  $F$  due to the factor  $A_{a,b}$  in  $\Delta(F)$ . Therefore, we can only apply [28, Theorem 2] which guarantees that  $\bar{\rho}_{F,p}$  is irreducible when  $p > (1 + 3^{18})^2$ . This bound is insufficient for our purposes.

The following combines the multi-Frey technique with Mazur like results to establish a much better irreducibility bound for  $\bar{\rho}_{F,p}$ .

**Theorem 8.** *Let  $d \geq 1$  be an integer such that all its prime factors  $\ell$  satisfy  $\ell \not\equiv 1 \pmod{13}$ . Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.2) with  $r = 13$  and exponent  $p \geq 5$ ,  $p \neq 13, 17, 37$ . Then  $\bar{\rho}_{F,p}$  is irreducible.*

*If in addition  $3 \mid d$  then  $\bar{\rho}_{F,p}$  is irreducible for all  $p \geq 5$ ,  $p \neq 13$ .*

*Proof.* Suppose  $\bar{\rho}_{F,p}$  is reducible, that is,

$$\bar{\rho}_{F,p} \sim \begin{pmatrix} \theta & \star \\ 0 & \theta' \end{pmatrix} \quad \text{with} \quad \theta, \theta' : G_K \rightarrow \mathbb{F}_p^* \quad \text{satisfying} \quad \theta\theta' = \chi_p.$$

We note that  $K = \mathbb{Q}(z)$ , where  $z^3 + z^2 - 4z + 1$ . According to the notation of [28, Theorem 1] we set  $\epsilon_1 = z$  and  $\epsilon_2 = 1 - z$ , observe that the unit group of  $K$  is generated by  $\{-1, \epsilon_1, \epsilon_2\}$  and compute  $B = 1$ . Thus from the first paragraph of the proof of [28, Theorem 1] we conclude that for  $p = 11$  and  $p \geq 17$  exactly one of  $\theta, \theta'$  ramifies at  $p$ . Since 7 is inert in  $K$  and  $F$  is semistable at 7, it follows from [32, Lemma 1] also that only one of  $\theta, \theta'$  ramifies at  $p = 7$ .

The characters  $\theta$  and  $\theta'$  ramify only at  $p$  and additive primes of  $F$ ; the latter are  $\mathfrak{p}_{13}$  and 2 when  $s = 3, 4$  (see (7.7)). Furthermore, at an additive prime  $\mathfrak{q}$  both  $\theta, \theta'$  have conductor exponent equal to  $v_{\mathfrak{q}}(N_F)/2$ ; in particular,  $s \neq 3$ .

Replacing  $F$  by a  $p$ -isogenous curve we can assume  $\theta$  is unramified at  $p$ . Therefore, the possible conductors of  $\theta$  are  $\mathfrak{p}_{13}$  or  $2^2\mathfrak{p}_{13}$  when  $s = 4$ . Let  $\infty_1, \infty_2$  and  $\infty_3$  be the real places of  $K$ . The Ray class groups for the modulus  $\mathfrak{p}_{13}\infty_1\infty_2\infty_3$  and  $2^2\mathfrak{p}_{13}\infty_1\infty_2\infty_3$  are isomorphic to

$$\mathbb{Z}/4\mathbb{Z} \quad \text{and} \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

respectively; hence  $\theta$  has order  $n = 1, 2$  or 4.

Suppose  $n = 1, 2$ . Thus either  $F$  or a quadratic twist  $F'$  of  $F$  has a  $p$ -torsion point defined over  $K$ . Note that  $F$  has full 2-torsion over  $K^+$  which is a quadratic extension of  $K$ , hence it has at least one 2-torsion point over  $K$ . Thus, the quadratic twist  $F'$  also has (at least) a 2-torsion point over  $K$  and we conclude that the  $K$ -torsion subgroup of  $F$  or  $F'$  has order divisible by  $2p$  with  $p \geq 7$ . From [11, Theorem 5], we see that this is impossible.

In particular, this proves the result for all primes  $p \equiv 3 \pmod{4}$ , because  $n = 4$  does not divide the order of  $\mathbb{F}_p^*$ .

Suppose  $n = 4$ . Since  $K^+$  is the field fixed by  $\theta^2$  (note  $\theta^2$  has conductor  $\mathfrak{p}_{13}$ ) and thus  $\theta$  has order 2 over  $K^+$ . After a quadratic twist, now over  $K^+$ , we conclude that  $F$  has a  $p$ -torsion point defined over  $K^+$ . From [21] we see this is possible only for  $p \leq 19$  and  $p = 37$ . We conclude that  $\bar{\rho}_{F,p}$  is irreducible for all  $p \geq 7$  such that  $p \neq 13, 17, 37$  (after discarding the primes  $p \equiv 3 \pmod{4}$ ).

The case  $p = 5$  follows from Lemma 4, completing the proof of the first statement.

Suppose now  $3 \mid d$  and  $p \neq 13$ . From Theorem 7, we can assume  $13 \mid a + b$  and  $4 \mid a + b$  (the conclusion of Theorem 7 holds also for  $3 \mid d$  using exactly the same proof). From (7.7), the conductor of  $F$  at 2 is  $2^s$  for  $s = 0, 1$  and  $F$  has potentially multiplicative reduction at  $\mathfrak{p}_{13}$ . This implies, after at most a quadratic twist, that the conductor of  $\bar{\rho}_{F,p}$  divides  $2^s\mathfrak{p}_{13}$  with  $s = 0, 1$ . Arguing as above, it follows that  $\theta$  ramifies only at the infinite places of  $K$  (since  $p \neq 13$ ), but  $K$  has narrow class group 1, so  $\theta = 1$ . As above,  $F$  has a  $2p$ -torsion point over  $K$  which is impossible for  $p \geq 7$ , again by [11, Theorem 5].  $\square$

**Lemma 4.** *Let  $d \geq 1$  be an integer such that all its prime factors  $\ell$  satisfy  $\ell \not\equiv 1 \pmod{13}$ . Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.2) with  $r = 13$  and  $p = 5$ .*

*Then  $\bar{\rho}_{F,5}$  is irreducible.*

*Proof.* We proceed using explicit equations as in [18, Theorem 7]. Let  $j_F$  denote the  $j$ -invariant of  $F$ . Then

$$\begin{aligned} j_F - 1728 &= \beta G(a, b)^2 / H(a, b)^2, \\ &= 13(\alpha G(a, b) / H(a, b))^2, \end{aligned}$$

where  $G(a, b), H(a, b) \in K[a, b]$  are monic, and  $\alpha, \beta \in K$ . If  $\bar{\rho}_{F,5}$  is reducible, that is,  $F$  has a 5-isogeny over  $K$ , then we must have that

$$j_F - 1728 = \frac{(t^2 + 4st - s^2)^2(t^2 + 22st + 125s^2)}{s^5t},$$

for some  $u = t/s \in \mathbb{P}^1(K)$ , following the argument in *loc. cit.* Thus, we obtain a  $K$ -rational point on the elliptic curve

$$D : 13Y^2 = (X^2 + 22X + 125)X,$$

where

$$\begin{aligned} X &= t/s = u, \\ Y &= \alpha \frac{G(a, b)}{H(a, b)} \frac{u}{u^2 + 4u - 1}. \end{aligned}$$

The elliptic curve  $D$  has rank 1 over  $K$  and over  $\mathbb{Q}$  and  $D_{tors}(K) = D_{tors}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$  [6]. This implies that  $D(K) = D(\mathbb{Q})$ , i.e. every  $K$ -rational point of  $D$  is in fact  $\mathbb{Q}$ -rational. Thus,

$$\alpha \frac{G(a, b)}{H(a, b)} \in \mathbb{Q},$$

which in turn implies that  $j_F - 1728 \in \mathbb{P}^1(\mathbb{Q})$ . It can be verified that this is not the case for  $a/b \in \mathbb{P}^1(\mathbb{Q})$ , except for  $a/b = -1$  [6].  $\square$

*Remark 7.8.* In the previous irreducibility proofs we could have tried to apply [11, Theorem 1] to cover the primes  $p = 5, 17, 37$  which, in case of success, would not require the hypothesis  $3 \mid d$ . However, it would require a more involved proof and it seems to only succeed for  $p = 17$ . Moreover, the following example shows that in the previous proof it is essential to be working with  $j$ -invariants arising from the Frey curve  $F$ . Consider the elliptic curve over  $\mathbb{Q}$  defined by

$$y^2 + (1 + a)xy + ay = x^3 + ax^2, \quad a = \frac{-10933}{144}$$

which has 10-torsion over  $\mathbb{Q}$  and acquires full 2-torsion over  $\mathbb{Q}(\sqrt{13})$ . In particular, it also has 10-torsion over  $K$  and a  $C_2 \times C_{10}$  torsion group over  $K^+$ .

From (7.7) and level lowering again, we obtain the following lemma.

**Lemma 5.** *Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.4) for exponent  $p \geq 5$ ,  $p \neq 13$ . Write  $F = F_{a,b}$ . Then,*

$$(7.9) \quad \bar{\rho}_{F,p} \cong \bar{\rho}_{f,\mathfrak{p}},$$

where  $f$  is an Hilbert newform over  $K$  of parallel weight 2, trivial character and level

$$N_f = 2^s \mathfrak{p}_{13}^2 \mathfrak{p}_3, \quad \text{where } s \in \{0, 1, 3, 4\}.$$

Furthermore, if  $4 \nmid a + b$  then  $s = 3, 4$  and if  $4 \mid a + b$  then  $s = 0, 1$ .



We now comment on the sizes of the spaces occurring in Lemma 5. The levels are  $N_f = 2^s \mathfrak{p}_{13}^2 \mathfrak{p}_3$  for  $s = 0, 1, 3, 4$  and with **Magma**, we check the corresponding dimensions of the cuspidal and new subspaces at each level. We respectively obtain:

$$\begin{aligned} s = 0: & 425, 334, \\ s = 1: & 3823, 2353, \\ s = 3: & 244609, 148101, \\ s = 4: & 1956865, 1184820. \end{aligned}$$

We see that for  $s = 0$  and  $s = 1$ , the computations of the newforms is within reach of current implementations (indeed, we have already computed a larger space when studying the case of  $r = 5$ ), but for  $s = 3$  and  $s = 4$ , the dimensions are totally out of reach. Using the multi-Frey technique, we are able to prove Theorem 2 by computing only in the cases  $s = 0, 1$ .

**7.3. Proof of Theorem 2.** The case  $p = 2$  follows from [2, Theorem 1.1] and the case  $p = 3$  follows from [4, Theorem 1.5].

For exponent  $p = 13$  the result follows from Theorem 2 in [40, Section 4.3]. Suppose  $(a, b, c)$  is a non-trivial primitive solution to (1.4) with  $p \geq 5$ ,  $p \neq 13$ . From Theorem 7 we can assume that

$$4 \mid a + b \quad \text{and} \quad 13 \mid c.$$

Write  $F = F_{a,b}$ . Lemma 5 implies that  $\bar{\rho}_{F,p} \cong \bar{\rho}_{f,\mathfrak{p}}$ , where  $f$  has level  $N_f = 2^s \mathfrak{p}_{13}^2 \mathfrak{p}_3$  with  $s = 0, 1$ . (Note that the multi-Frey technique is implicit in this step because the proof of Theorem 7 uses the Frey curve  $E$ .)

Since  $13 \mid c$ , or equivalently  $13 \mid a + b$ , we see that  $F$  has potentially multiplicative reduction at  $\mathfrak{p}_{13}$  and its quadratic twist by 13, denoted  $F'$ , has multiplicative reduction. Therefore,  $\bar{\rho}_{F',p} \cong \bar{\rho}_{g,\mathfrak{p}}$ , where  $g$  is a newform of level  $N_g = 2^s \mathfrak{p}_{13} \mathfrak{p}_3$  with  $s = 0, 1$ .

Note that the quadratic twist reduced the dimension of the spaces we actually need to compute even further; indeed, for  $s = 0$  the dimensions of the cuspidal and new subspaces are respectively 33, 27; and for  $s = 1$  they are 295, 181. Using [6], we compute all the newforms  $g$  in these spaces and bound the exponent using the primes in  $K$  above rational primes 5, 7, 11, 17, 31 using a similar method to §4.3, discarding all newforms for  $p > 13$ . For  $s = 1$ , there are 4, 5, 2 forms which we cannot eliminate for the exponents  $p = 5, 7, 11$ , respectively. For  $s = 0$ , there are 1, 3 forms which we cannot eliminate for the exponents  $p = 5, 7$ , respectively. Observe however, for  $s = 0$ , we may further use the trace of Frobenius at 2; this succeeds in eliminating two of the surviving forms for  $p = 7$ .

To deal with the remaining forms and exponents, we use the following refined elimination technique, which we illustrate for the exponent  $p = 11$ .

There are two forms  $f_i$ ,  $i = 1, 2$ , at level  $N_g = 2 \mathfrak{p}_{13} \mathfrak{p}_3$  which we cannot eliminate if  $p = 11$ . This is because the quantities to  $q\mathcal{F}_q(f_i)$  are divisible by 11 for each rational prime  $q$  up to 40. This means we could have  $\bar{\rho}_{F',11} \cong \bar{\rho}_{f_i,\mathfrak{p}}$  for some prime  $\mathfrak{p} \mid 11$  in the field of coefficients of  $f_i$ , so we assume this is the case.

Suppose that  $5 \nmid a + b$ , so that  $F'$  has good reduction at the three primes  $\mathfrak{q}_j \mid 5$  in  $K$ . Thus, taking the traces at the corresponding Frobenius, we obtain

$$a_{\mathfrak{q}_j}(f_i) \equiv a_{\mathfrak{q}_j}(F') \pmod{\mathfrak{p}} \quad \Leftrightarrow \quad a_{\mathfrak{q}_j}(f_i) - a_{\mathfrak{q}_j}(F') \equiv 0 \pmod{\mathfrak{p}}$$

for  $j = 1, 2, 3$  simultaneously. We check using [6] that this is not the case for *every* prime  $\mathfrak{p}$  above 11 in the field of coefficients of  $f_i$  for  $i = 1, 2$ .

Suppose that  $5 \mid a + b$ , so that  $F'$  has multiplicative reduction at  $\mathfrak{q}_j$  for  $j = 1, 2, 3$ . Thus, the level raising condition at  $\mathfrak{q}_j \nmid p$  implies that, for some choice of sign for each  $j$ ,

$$a_{\mathfrak{q}_j}(f_i) \equiv \pm(N(\mathfrak{q}_j) + 1) = \pm 6 \pmod{\mathfrak{p}} \Rightarrow a_{\mathfrak{q}_j}(f_i)^2 - 6^2 \equiv 0 \pmod{\mathfrak{p}}$$

for  $j = 1, 2, 3$  simultaneously. Again, using [6], we check this is not possible for  $i = 1, 2$ .

We proceed similarly for the remaining forms and exponents by using the auxiliary primes  $q = 5$  or  $q = 31$ , which succeeds in eliminating all of them.

## REFERENCES

- [1] Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani. On the equation  $a^3 + b^{3n} = c^2$ . *Acta Arith.*, 163(4):327–343, 2014. [3](#)
- [2] Michael A. Bennett and Christopher Skinner. Ternary diophantine equations via galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004. [1](#), [3](#), [4.4](#), [5.1](#), [6](#), [7.3](#)
- [3] Michael A. Bennett, V. Vatsal, and S. Yazdani. Ternary diophantine equations of signature  $(p, p, 3)$ . *Compositio Math.*, 140(1):1399–1416, 2004. [1](#)
- [4] Michael A. Bennett, Vinayak Vatsal, and Soroosh Yazdani. Ternary Diophantine equations of signature  $(p, p, 3)$ . *Compos. Math.*, 140(6):1399–1416, 2004. [4.4](#), [5.1](#), [6](#), [7.3](#)
- [5] Nicolas Billerey. Equations de Fermat de type  $(5, 5, p)$ . *Bull. Austral. Math. Soc.*, 76(2):161–194, 2007. [1.1](#), [4.1](#), [4.1](#), [4.4](#), [5.1](#), [6](#)
- [6] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas. Supporting Magma program files for this paper. [1.1](#), [4.2](#), [4.3](#), [5.1](#), [5.2](#), [6](#), [7.1](#), [7.1](#), [7.2](#), [7.2](#), [7.3](#)
- [7] Nicolas Billerey and Luis V. Dieulefait. Solving Fermat-type equations  $x^5 + y^5 = dz^p$ . *Math. Comp.*, 79(269):535–544, 2010. [1.1](#), [4.1](#), [4.1](#)
- [8] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). [1.1](#)
- [9] Christophe Breuil. Sur quelques représentations modulaires et  $p$ -adiques de  $\mathrm{GL}_2(\mathbb{Q}_p)$ , II. *J. Inst. Math. Jussieu*, 2:1–36, 2003. [6](#)
- [10] Christophe Breuil and Ariane Mézard. Multiplicités modulaires et représentations de  $\mathrm{GL}_2(\mathbb{Z}_p)$  et de  $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$  en  $\ell = p$  (with an appendix by G. Henniart). *Duke Math. J.*, 115:205–310, 2002. [6](#)
- [11] Peter Bruin and Filip Najman. A criterion to rule out torsion groups for elliptic curves over number fields. *Research in Number Theory*, 2:1–12, 2016. [7.2](#), [7.8](#)
- [12] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek. Almost powers in the Lucas sequence. *J. Théor. Nombres Bordeaux*, 20(3):555–600, 2008. [1](#), [2](#)
- [13] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Classical and modular methods to exponential diophantine equations II: The Lebesgue-Nagell equation. *Compositio Mathematica*, 142:31–62, 2006. [1](#)
- [14] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Classical and modular methods to exponential diophantine equations I. Fibonacci and Lucas perfect powers. *Annals of Mathematics*, 163:969–1018, 2006. [1](#)
- [15] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. A multi-Frey approach to some multi-parameter families of Diophantine equations. *Canad. J. Math.*, 60(3):491–519, 2008. [1](#), [2](#)
- [16] José I. Burgos and Ariel Pacetti. Hecke and sturm bounds for hilbert modular forms over real quadratic fields. [7.6](#)
- [17] Élie Cali. Défaut de semi-stabilité des courbes elliptiques dans le cas non ramifié. *Canad. J. Math.*, 56(4):673–698, 2004. [4.2](#), [4.4](#)
- [18] Sander R. Dahmen. A refined modular approach to the Diophantine equation  $x^2 + y^{2n} = z^3$ . *Int. J. Number Theory*, 7(5):1303–1316, 2011. [7.2](#)

- [19] Henri Darmon and Andrew Granville. On the equations  $z^m = f(x, y)$  and  $ax^p + by^q = cz^r$ . *Bull. London Math. Soc.*, 27(6):513–543, 1995. [1](#)
- [20] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat’s Last Theorem. *J. Reine Angew. Math.*, 490:81–100, 1997. [5.1](#), [6](#)
- [21] M. Derickx, S. Kamienny, W. Stein, and M. Stoll. Torsion points on elliptic curves over number fields of small degree. (in preparation). [1.1](#), [7.2](#)
- [22] Luis Dieulefait and Nuno Freitas. Fermat-type equations of signature  $(13, 13, p)$  via Hilbert cuspforms. *Math. Ann.*, 357(3):987–1004, 2013. [1](#), [1.1](#), [7.1](#), [7.1](#), [7.1](#), [7.1](#)
- [23] Luis Dieulefait and Nuno Freitas. The Fermat-type equations  $x^5 + y^5 = 2z^p$  or  $3z^p$  solved through  $\mathbb{Q}$ -curves. *Math. Comp.*, 83(286):917–933, 2014. [1.1](#), [4.2](#), [4.2](#), [4.2](#), [4.4](#), [4.11](#)
- [24] L. Dirichlet. Mémoire sur l’impossibilité de quelques équations indéterminées du cinquième degré. *J. reine angew. Math.*, 3:354–375, 1828. [4.4](#)
- [25] Jordan S. Ellenberg. Galois representations attached to  $\mathbb{Q}$ -curves and the generalized Fermat equation  $A^4 + B^2 = C^p$ . *Amer. J. Math.*, 126(4):763–787, 2004. [4.2](#)
- [26] Nuno Freitas. Recipes to Fermat-type equations of the form  $x^r + y^r = Cz^p$ . *Math. Z.*, 279(3-4):605–639, 2015. [1.1](#), [4.3](#), [4.7](#), [7.2](#), [7.2](#)
- [27] Nuno Freitas, Bao V. Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular. *Invent. Math.*, 201(1):159–206, 2015. [4.2](#), [4.2](#), [7.1](#)
- [28] Nuno Freitas and Samir Siksek. Criteria for irreducibility of  $\text{mod } p$  representations of Frey curves. *Théor. Nombres Bordeaux*, 27(1):67–76, 2015. [1.1](#), [7.1](#), [7.2](#), [7.2](#)
- [29] Kazuhiro Fujiwara. Level optimization in the totally real case. *arXiv:0602586v1*, 27 February 2006. [4.2](#), [7.1](#)
- [30] Frazer Jarvis. Level lowering for modular  $\text{mod } \ell$  galois representations over totally real fields. *Mathematische Annalen*, 313:141–160, 1999. [4.2](#)
- [31] Frazer Jarvis. Correspondences on Shimura curves and Mazur’s principle at  $p$ . *Pacific J. Math.*, 213(2):267–280, 2004. [4.2](#), [7.1](#)
- [32] Alain Kraus. Courbes elliptiques semi-stables et corps quadratiques. *Journal of Number Theory*, 60:245–253, 1996. [7.2](#)
- [33] Alain Kraus. Majorations effectives pour l’équation de Fermat généralisée. *Canadian J. Math.*, 49:1139–1161, 1997. [1](#)
- [34] Alain Kraus. Sur l’équation  $a^3 + b^3 = c^p$ . *Experiment. Math.*, 7:1–13, 1998. [1](#)
- [35] The LMFDB Collaboration. The L-functions and modular forms database. <http://www.lmfdb.org>, 2013. [Online; accessed 16 September 2013]. [4.1](#)
- [36] David Loeffler and Jared Weinstein. On the computation of local components of a newform. *Math. Comp.*, 81(278):1179–1200, 2012. [3.4](#)
- [37] David Loeffler and Jared Weinstein. Erratum: “On the computation of local components of a newform” [mr2869056]. *Math. Comp.*, 84(291):355–356, 2015. [3.4](#)
- [38] Ali Rajaei. On the levels of  $\text{mod } \ell$  Hilbert modular forms. *J. Reine Angew. Math.*, 537:33–65, 2001. [4.2](#), [7.1](#)
- [39] Kenneth A. Ribet. On the equation  $a^p + 2^\alpha b^p + c^p = 0$ . *Acta Arith.*, 79:7–16, 1997. [1](#)
- [40] J.-P. Serre. Sur les représentations modulaires de degré 2 de  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . *Duke Math. J.*, 54:179–230, 1987. [1](#), [7.3](#)
- [41] Andrew Wiles. Modular elliptic curves and Fermat’s Last Theorem. *Annals of Mathematics*, 144:443–551, 1995. [1](#)

UNIVERSITÉ CLERMONT AUVERGNE, CNRS, LMBP, F-63000 CLERMONT-FERRAND, FRANCE.

*E-mail address:* `Nicolas.Billerey@math.univ-bpclermont.fr`

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, BURNABY, BC V5A 1S6, CANADA

*E-mail address:* `ichen@sfu.ca`

DEPARTAMENT D'ALGEBRA I GEOMETRIA, UNIVERSITAT DE BARCELONA, G.V. DE LES CORTS CATALANES  
585, 08007 BARCELONA, SPAIN

*E-mail address:* `ldieulefait@ub.edu`

UNIVERSITY OF BRITISH COLUMBIA, DEPARTMENT OF MATHEMATICS, VANCOUVER, BC V6T 1Z2 CANADA

*E-mail address:* `nunobfreitas@gmail.com`